Client  
Revue générale informatique

# Les applications

|  |  |  |
| --- | --- | --- |
| **Application (fournisseur)** | **Fonctions** | **Remarques** |
| Gestion commerciale CCMX |  |  |
| Achats GP CIEL |  |  |
| Paye SAGE 100 |  |  |
| Comptabilité SAGE 100 |  |  |
| Immobilisation SAGE 100 |  |  |

**Légende :**

|  |  |
| --- | --- |
|  | Interface automatique |
|  | Interface semi-automatique (intervention d’export et /ou d’import) |
|  | Interface manuelle (ressaisie) |

# Liaisons entre applications

Immobilisation SAGE 100

Comptabilité SAGE 100

Trésorerie ZZ

Ventes CCMX

Paie SAGE 100

Achat & stock CIEL

………………..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Liaison** exp : Paie🢧comptabilité | **Type : M/S/A (1)** | **Fréquence (M,H,Q)(2)** | **Nature des contrôles  (manuels ou automatisés)** | **Risque (I/M/F)(3)** |
| Ciel => Compta | A | Q | Ctrl bouclage mensuel (formalisé et archivé) | F |
| Ventes => compta | S | Q | Att manipulation de fichiers non contrôlée. Bouclage annuel | M |
| Paie => compta | S | M | Bouclage livre paie // journal paie | F |
| IMMO => compta | S | A | Bouclage totaux 2054-2055// journal amort | F |

1. M = interface manuel ; S = semi-automatique c'est-à-dire intervention d’un utilisateur ; A = automatique aucune intervention.
2. Annuel, Mensuel, Hebdomadaire, Quotidien
3. Important, Moyen, Faible

# L’équipe informatique

|  |  |  |
| --- | --- | --- |
| **Personne** | **Téléph.** | **Fonction** |
|  |  | Directeur / responsable informatique |
|  |  | Technicien réseau |

# Les infrastructures

|  |  |
| --- | --- |
| Système d’exploitation des postes |  |
| Système d’exploitation des serveurs |  |

|  |  |
| --- | --- |
| **Les serveurs** | **Utilisation** |
| S1 |  |
| S2 |  |

# Besoin de sécurité – exigence de disponibilité

|  |  |  |  |
| --- | --- | --- | --- |
| Cycle | Application // serveurs | disponibilité (J) | Obs. |
| Achat |  |  |  |
| Vente |  |  |  |
| Production |  |  |  |

**Rappel** : l’exigence recherchée tient compte des contraintes suivantes :

* Engagements client, fournisseurs, tiers (si pas de marge de manœuvre)
* Contraintes réglementaires
* Fonctionnent de l’entreprise à la limite du supportable et du vital.

# Revue de Sécurité

| **Ref** | **Point de contrôle** | **Forces** | **Faiblesses** |
| --- | --- | --- | --- |
|  | Historique de l'informatique de la société |  | |
| **1** | **Sécurité physique** |  | |
| **1.1** | **Infrastructures physiques** |  |  |
|  | Qualité des murs et fenêtres |  |  |
|  | Risque étanchéité / inondation |  |  |
|  | Détection intrusion (alarme gardiennage) |  |  |
|  | Organisation des locaux informatiques & télécom |  |  |
| **1.2** | **Protection incendie** |  |  |
|  | Dispositif détection / extinction |  |  |
|  | Entretien équipements |  |  |
|  | Remonté des alarmes |  |  |
| **1.3** | **Protection électrique** |  |  |
|  | Onduleur batterie sur chaque serveur |  |  |
|  | Test fonction « on line » |  |  |
| **1.4** | **Climatisation / Réfrigération** |  |  |
|  | Dispositif & Entretien équipements |  |  |
| **1.5** | **Contrôle des accès** |  |  |
|  | Contrôle d’accès de l’entreprise (jour / nuit ) |  |  |
|  | Contrôle d’accès zone informatique (jour / nuit ) |  |  |
| **1.6** | **Conditions d'hygiène** |  |  |
|  | Murs & plancher |  |  |
|  | Rangement des locaux info. |  |  |
|  | Proximité d’autres risques |  |  |
| **1.7** | **Maintenance du matériel** |  |  |
|  | Un contrat pour chaque serveur de production auprès d’un professionnel |  |  |
| **1.8** | **Contrat d'assurance des biens informatiques** |  |  |
|  | Maj de l’inventaire |  |  |
|  | Exclusions |  |  |
| **D1.9** | **Plan de back-up** |  |  |
|  | Organisation & documentation |  |  |
|  | Tests |  |  |
| **D2** | **Sécurité logique** |  | |
| **2.1** | **Contrôle d’accès logique** |  |  |
|  | Description des outils de contrôle d’accès |  |  |
|  | Procédure d’habilitation : formalisation, Attribution, Révocation |  |  |
|  | user-id et Mdp individuels |  |  |
|  | Renouvellement et Mdp |  |  |
|  | Organisation des groupes utilisateurs |  |  |
|  | Contrôles a posteriori de l’utilisation des transactions |  |  |
| **2.2** | **Sécurité du poste de travail** |  |  |
|  | Anti-virus sur serveur et Postes |  |  |
|  | Mise à jour Anti-virus |  |  |
|  | Écran de veille installé sur chaque pc / serveur |  |  |
|  | Extinction PC soir et WE |  |  |
|  | Sensibilisation des utilisateurs – charte et formation |  |  |
| **2.3** | **Séparation des environnements études / exploitation** |  |  |
| **2.4** | **Limitation des accès aux utilitaires et fichiers système** |  |  |
| **2.5** | **Limitation des accès aux transactions** |  |  |
| **2.6** | **Sécurité des accès Internet** |  |  |
| **3** | **Conditions d'exploitation** |  | |
|  | Contexte général |  | |
|  | Planification et suivi de l'exploitation |  |  |
|  | Contrôle de la planification |  |  |
|  | Contrôle de l'exécution des traitements |  |  |
|  | Gestion des incidents d'exploitation |  |  |
|  | Contrôle des traitements |  |  |
|  | Procédure de Mise en production |  |  |
|  | Flux de données et interfaces |  |  |
|  | Suivi des espaces disques |  |  |
|  | Archivage et purge des données |  |  |
| **4** | **Procédure de sauvegarde** |  | |
|  | Description générale |  | |
|  | Déclenchement auto / manuel |  |  |
|  | Stockage externe |  |  |
|  | Contrôle de relecture des supports |  |  |
|  | Contrôle nbr d’utilisation des supports |  |  |
|  | Labellisation des supports |  |  |
|  | Maj du périmètre |  |  |
|  | Sauvegarde des données des postes (PC) du réseau |  |  |

**Organisation des sauvegardes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cycle** | **Contenu** (OS, data, appli,….) | **Nbr Jeux** | **Stockage** (lieu, accès, conditions température, …) |
| Quotidienne |  |  |  |
| Hébdo |  |  |  |
| Mensuelle |  |  |  |
| Annuelle |  |  |  |

| **Ref** | **Point de contrôle** | **Forces** | **Faiblesses** |
| --- | --- | --- | --- |
| **5** | **Méthodologie de développement des applications** |  | |
|  | Méthode projet |  |  |
|  | Méthode programmation |  |  |
|  | Méthode test |  |  |
|  | Perspectives d’évolution |  |  |

| **Ref** | **Point de contrôle** | **Forces** | | **Faiblesses** |
| --- | --- | --- | --- | --- |
| **6** | **Contraintes légales** |  | | |
| **6.1** | **Loi informatique et liberté du 6/1/78** |  | |  |
|  | Recensement et déclaration des fichiers : | | Déclaré | Non déclaré |
|  | Clients pers et prospects (N°48)  Suivi des temps individuel  Suivi médical et formation du personnel (N°46)  Log des connexions Internet (N° 46)  Taxateur téléphonique et messagerie (N° 47)  Contrôle d’accès, restauration, parking, visiteurs (N°42)  habilitation et accès SI (N°46) | |  |  |
|  | Mentions obligatoires lors de la collecte (art 32 loi 78-17) |  | |  |
|  | Loi 85-660 du 3/07/85 relative à la protection des logiciels – politique d’achat de licences |  | |  |
| **6.2** | **CFCI contrôles généraux** |  | |  |
|  | Appréciation du niveau d’archivage détaillé |  | |  |
|  | Date et mode de déclenchement de l’archive fiscale |  | |  |
|  | Existence d’un « pilote » CFCI |  | |  |
|  | Test de la production du FEC |  | |  |

**CFCI contrôles applicatifs**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application (fournisseur)** | **Existence doc tech [[1]](#footnote-1)** | **Existence doc utilisateurs[[2]](#footnote-2)** | **Piste d’audit comptable[[3]](#footnote-3)** | **Purge/ agrégation[[4]](#footnote-4)** | **Accès source[[5]](#footnote-5)** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

| **Ref** | **Point de contrôle** | **Forces** | **Faiblesses** |
| --- | --- | --- | --- |
| **7** | **Stratégie et pilotage** |  | |
| **7.1** | Une stratégie est définie pour le SI : |  |  |
|  | Implication de la DG |  |  |
|  | Architecture technique et réseau |  |  |
|  | Prise en compte des besoins utilisateurs |  |  |
|  | Evaluation et suivi des risques |  |  |
|  | Définition d’une politique de sécurité |  |  |
| **7.2** | Les Outils de pilotage |  |  |
|  | Au travers de réunions régulières |  |  |
|  | Grâce à l’utilisation d’un tableau de bord |  |  |

1. Structure des données, modalités d’exportation, accès à la base de données [↑](#footnote-ref-1)
2. Présentation générale de l’application, description des écrans et des traitements, des codifications [↑](#footnote-ref-2)
3. Chaque évènement de gestion dispose d’une référence unique et stable qui figure en référence de la pièce comptable sui en résulte PCG 420-2 [↑](#footnote-ref-3)
4. Existence de purge des données avant archivage annuel [↑](#footnote-ref-4)
5. Possibilité de présenter les programmes sources à l’Administration [↑](#footnote-ref-5)